Thomas Schneck
David M. Schneck
Gina McCarthy
Nissa Strottman

Law Offices of
SCHNECK & SCHNECK

P.O. BOX 2-E
SAN JOSE, CALIFORNIA 95109-0005

80 S. Market Street
Third Floor
San Jose, California 95113-2303

Email: mail@patentvalley.com

Telephone: (408) 297-9733

Facsimile: (408) 297-9748

Patents and Trademarks

August 22, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Re: Certified Copy of Priority Document
U.S. Serial No.: 10/615,476
Filed: July 7, 2003
For: COMBINED POLYNOMIAL AND NATURAL MULTIPLIER ARCHITECTURE
Our ref: ATM-213 (V. Dupaquis et al.)

Dear Sir:

Transmitted herewith for the above-identified patent application is a certified copy of the priority document, French application no. 03/04221 filed April 4, 2003.

Respectfully submitted,

Thomas Schneck

Reg. No. 24,518

Schneck & Schneck
P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Signed: Merle P. Garcia
Typed Name: Merle P. Garcia

Date: August 22, 2003

Encl: Certified copy of priority document
cc: J. McGuire, Esq. w/encl.

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 27 JUIN 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*02

REQUÊTE EN DÉLIVRANCE page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 010801

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 4 AVRIL 2003
75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0304221
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI - 4 AVR. 2003

Vos références pour ce dossier *(facultatif)* 33299/FR

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

BREESE-MAJEROWICZ
3 avenue de l'Opéra
75001 PARIS

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes	
Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 **TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

ARCHITECTURE DE MULTIPLICATEURS POLYNOMIAL ET NATUREL COMBINES

4 **DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE**

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases)		☒ Personne morale ☐ Personne physique
Nom ou dénomination sociale		Atmel Corporation
Prénoms		
Forme juridique		constituée selon les lois de l'État du Delaware
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	2325 Orchard Parkway
	Code postal et ville	SAN JOSE California 95131
	Pays	U.S.A.
Nationalité		U.S.A.
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case t utilisez l'imprimé «Suit »**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 4 AVRIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0304221

DB 540 @ W / 010801

Vos références pour ce dossier : *(facultatif)*		33299/FR
6 MANDATAIRE *(s'il y a lieu)*		
Nom		BREESE
Prénom		Pierre
Cabinet ou Société		BREESE-MAJEROWICZ
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	3 avenue de l'Opéra
	Code postal et ville	7 5 0 0 1 Paris
	Pays	France
N° de téléphone *(facultatif)*		01 47 03 67 77
N° de télécopie *(facultatif)*		01 47 03 67 78
Adresse électronique *(facultatif)*		office@breese.fr
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur pr pr d´pôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
BREESE Pierre

921038

VISA DE LA PRÉFECTURE OU DE L'INPI

M. MARTIN

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

ARCHITECTURE DE MULTIPLICATEURS POLYNOMIAL ET NATUREL COMBINES

La présente invention concerne des architectures de circuits intégrés à semi-conducteurs, en particulier des circuits de multiplication.

Le matériel de multiplication est habituellement adapté pour effectuer une multiplication naturelle (la multiplication arithmétique normale enseignée à l'école primaire), mais sur des nombres binaires. Dans une multiplication naturelle, deux opérandes A et B sont multipliés l'un par l'autre afin de former un produit C = A.B, où A, B et C sont représentés par des nombres binaires a_i, b_j et c_k égaux à 0 ou 1 :

$$A = (a_{n-1}, \ldots, a_1, a_0) = SUM_i \ (a_i.2^i) \ ;$$
$$B = (b_{n-1}, \ldots, b_1, b_0) = SUM_j \ (b_j.2^j) \ ;$$
$$C = (c_{2n-1}, \ldots, c_1, c_0) = SUM_k \ (c_k.2^k).$$

Ici, les indices i, j et k représentent l'importance ou le « poids » binaire du chiffre particulier. (Des représentations de nombre similaires, telles que par complément à deux ou par complément à un, sont utilisées communément pour représenter des entiers négatifs, ainsi que la mantisse de nombres réels. Une multiplication utilisant ces autres représentations de nombre est également similaire, avec des modifications appropriées).

Dans des architectures de multiplicateurs parallèles, le produit est généralement formé comme une somme de produits croisés. Le produit partiel de deux bits d'opérande est équivalent à une opération ET logique

et peut être effectué dans un circuit matériel en utilisant des portes ET. La somme de deux bits de produit partiel de poids identique produit un terme de somme de même poids et un terme de retenue du poids supérieur suivant, où le terme de somme est équivalent à une opération OU Exclusif logique et le terme de retenue est équivalent à une opération ET logique :

$$x + y = \text{retenue, somme} = \text{AND}(x, y), \text{XOR}(x, y).$$

Généralement, les additionneurs matériels sont répartis en deux types principaux, les additionneurs complets qui additionnent trois bits d'entrée et les demi-additionneurs qui additionnent deux bits d'entrée. Les bits d'entrée pourraient être des bits de produit partiel, des termes de somme délivrés par un autre additionneur ou des termes de retenue. Tous les bits d'entrée qu'elle que soit leur origine, y compris les bits d'entrée de « retenue », ont exactement la même contribution logique aux sorties de l'additionneur et sont normalement traités comme étant équivalents vis-à-vis du résultat. (Notez, cependant, que les mises en oeuvre de cellule standard de circuits additionneurs donnent souvent aux entrées de retenue une synchronisation privilégiée dans la construction du circuit additionneur afin de réduire à un minimum les retards de propagation et une commutation excessive dans l'architecture d'ensemble d'additionneurs globale). Les deux types d'additionneurs produisent un terme de somme et un terme de retenue en tant que sorties.

Dans une multiplication naturelle, les termes de retenue se propagent et sont ajoutés aux termes de somme

de poids supérieur suivant. Ainsi, le produit naturel C est :

$$C = SUM_{i,j}\ (a_i.b_j.2^{i-j})$$
$$= SUM_k\ ((SUM_{i-j-k}\ (AND(a_i,\ b_j)))\ 2^k).$$

Les circuits multiplicateurs naturels parallèles existent en diverses architectures, qui diffèrent principalement par la manière d'agencer les ensembles d'additionneurs de produits partiels.

Les architectures de Wallace (de « A Suggestion for a Fast Multiplier », IEEE Trans. on Electronic Computers, vol. RC-15, pages 14 à 17, février 1964) et de Dadda (à partir d'un document présenté au Colloque sur l'Algèbre de Boole, Grenoble, France, janvier 1965) sont similaires. La structure de base présentée par L. Dadda est montrée sur la figure 1. L'ensemble de produits partiels est représenté par des points alignés dans la zone A dans les colonnes verticales conformément à leurs poids. Le nombre de produits partiels d'un poids donné peut varier de 1 à n pour deux opérandes de n bits. L'addition des produits partiels d'un poids donné est effectuée par des compteurs binaires, représentés sur la figure par des diagonales. Le terme « compteur binaire » est utilisé par Dadda et dans l'ensemble de ce document dans le sens où, pour un nombre donné de lignes d'entrée, il produit une sortie binaire représentant le nombre total ou le « compte » de 1 sur ces entrées. Ceci est différent du compteur séquentiel habituel qui produit une série de sorties incrémentées dans le temps. L'addition des produits partiels est divisée en deux étapes principales, dans lesquelles une première étape (sub-

divisée en plusieurs étages en cascade) réduit les produits partiels à un ensemble de deux nombres et une deuxième étape comprend un étage d'additionneur unique à propagation de retenue. Les étages en cascade de la première étape sont montrés sur la figure en tant que zones B à D. La dimension du compteur dépend du nombre total de termes d'un poids donné qui doivent être comptés. Par exemple, dans la zone B, colonne 5, il y a 5 produits partiels de poids 2^4 à ajouter (à compter), qui forment ensemble une somme de 3 bits respectivement de poids 2^6, 2^5, 2^4. Ainsi, il y a plusieurs termes de retenue de différents poids qui se propagent vers l'étage ou la zone de comptage suivant. Les zones C et D appliquent le même principe aux sorties de la zone précédente. La sortie des compteurs de la zone D est constituée de deux lignes seulement. Celles-ci sont traitées par des additionneurs rapides dans la deuxième étape principale (dans la zone E) pour obtenir le produit naturel. D'autres multiplicateurs naturels parallèles peuvent utiliser divers types de structures arborescentes d'additionneurs complets (ou même des circuits additionneurs plus complexes) pour réduire rapidement les produits partiels à un produit final.

D'autres types d'algèbre ont leur propre forme de multiplication. Un type communément utilisé pour la génération de codes de correction d'erreur, et plus récemment dans des systèmes cryptographiques à courbe elliptique (voir, par exemple, le brevet US n° 6 252 959) génère des produits de multiplication dans un domaine fini (Galois). Différents domaines peuvent être utilisés, mais les applications les plus communes utilisent soit des domaines de nombres premiers GF(p), soit des domaines

binaires $GF(2^N)$. Les applications à code de correction d'erreur, telles que la génération de code Reed-Solomon, opèrent généralement de manière répétée sur des mots de petite taille, par exemple de 8 bits, et pourraient ainsi utiliser une multiplication sur GF(256). Les applications à courbe elliptique opèrent généralement sur des blocs beaucoup plus grands avec des largeurs de mot de 160 bits ou plus. Souvent, dans l'une ou l'autre de ces applications, en utilisant une représentation polynomiale, le produit est défini comme un produit polynomial, est réduit par la suite à une division de données résiduelles par un polynôme irréductible approprié. Des architectures matérielles dédiées ont été réalisées pour mettre en oeuvre une multiplication à domaine fini.

Dans $GF(2^N)$, les éléments d'un nombre peuvent être représentés comme n uples (représentation matricielle) ou comme des polynômes avec n coefficients (représentation polynomiale) :

$$A = (a_{n-1}, \ldots, a_1, a_0) = a_{n-1}\, x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 = \mathrm{SUM}_i\ (a_i x^i).$$

Les a_i sont membre de GF(2), c'est-à-dire peuvent être 0 ou 1. Les lois d'addition et de multiplication sur GF(2) sont respectivement les opérations logiques OU Exclusif et ET. L'addition de deux nombres de $GF(2^N)$ est définie comme une addition polynomiale, c'est-à-dire une addition des coefficients de degré ou de poids identique :

$$C = A + B - \mathrm{SUM}_i\ (\mathrm{XOR}\ (a_i, b_i)\ x^i).$$

La multiplication de deux nombres de $GF(2^N)$ est définie comme une multiplication polynomiale, modulo un polynôme irréductible spécifique P :

$$C = A.B = (A * B) \bmod P$$
$$= SUM_k\ (XOR_{i+j-k}\ (AND\ (a_i, b_j))x^k) \bmod P,$$

avec k compris entre 0 et N - 1. Pour notation, A * B représente le produit polynomial (non réduit modulo P), tandis que A.B représente le produit de deux nombres de $GF(2^N)$. A * B est un polynôme de degré 2N - 2 et n'est donc pas un membre de $GF(2^N)$. A.B est un membre de $GF(2^N)$.

Lors de la comparaison de l'addition et de la multiplication polynomiales ayant des coefficients dans GF(2) avec une addition et une multiplication naturelles, nous constatons que a_kx^k (terme polynomial de degré k) et a_k2^k (bit de poids k d'un nombre naturel) jouent un rôle similaire dans l'addition et la multiplication, mais avec une certaine différence. L'addition polynomiale avec des coefficients dans le domaine fini GF(2) est similaire à celle pour une addition naturelle, excepté que la somme de termes de degré identique ne fournit aucune retenue pour des termes adjacents dans le cas d'une addition polynomiale, tandis que l'addition naturelle de termes de poids identique fournit une retenue au poids supérieur suivant. La multiplication polynomiale avec des coefficients dans le domaine fini GF(2) est également similaire à celle pour une multiplication naturelle, excepté que la somme de produits partiels de degré identique ne génère pas de retenues pour les degrés adjacents dans le cas d'une multiplication polynomiale,

tandis que la somme naturelle de produits partiels des termes de même poids fournit une retenue au poids supérieur suivant. Enfin, nous soulignons que le bit le moins significatif de la somme naturelle de n bits est un OU Exclusif de ces bits, exactement comme dans le cas polynomial.

Dans le brevet US n° 4 918 638, de Matsumoto et autres, décrivent un multiplicateur à domaine fini pour obtenir un produit dans $GF(2^4)$ destiné à être utilisé pour la génération de codes de correction d'erreur. Après avoir effectué une multiplication binaire, un bloc de générateur polynomial séparé réduit le produit par une division par un polynôme générateur $g(x) = x^a + x + 1$. Les figures 5 et 9 de ce brevet montrent des ensembles de multiplicateurs binaires pour effectuer la multiplication à domaine fini. Des portes ET sont utilisées pour former les produits partiels, tandis que des portes OU Exclusif sont utilisées pour effectuer l'addition de bits sur les produits partiels de même poids. Le multiplicateur n'est pas réalisé pour effectuer une multiplication naturelle, mais uniquement une multiplication à domaine fini $GF(2^4)$.

Un objet de la présente invention consiste à proposer des architectures de multiplicateurs parallèles qui sont capables de délivrer à la fois un produit de multiplication naturelle et un produit de multiplication polynomiale avec des coefficients sur GF(2), facilitant ainsi la réalisation d'une multiplication à domaine fini dans $GF(2^N)$ pour n'importe quelles valeurs de $N \geq 1$.

Cet objectif est satisfait par une architecture matérielle de multiplicateurs parallèles qui agence l'addition de produits partiels de sorte qu'elle commence

dans un premier groupe d'étages d'additionneurs qui effectuent des additions sans recevoir de termes de retenue en tant qu'entrées, et de sorte qu'une addition des termes de retenue soit différée jusqu'à un deuxième groupe d'étages d'additionneurs agencé pour suivre le premier groupe. Cet agencement intentionnel des additionneurs en deux groupes séparés permet à la fois l'extraction du produit polynomial des résultats du premier groupe d'additions et l'extraction du produit naturel des résultats du deuxième groupe d'additions.

Le multiplicateur comprend un ensemble de portes ET avec des entrées connectées à des bits d'opérande et avec des sorties délivrant un ensemble complet de produits partiels des bits d'opérande, chaque produit partiel étant caractérisé par une importance ou un « poids » de bit ; une architecture d'addition agencée pour additionner des produits partiels du même poids, l'architecture d'addition étant réalisée par des étages multiples, un premier groupe d'étages étant agencé pour additionner des produits partiels sans recevoir la moindre entrée de retenue d'une partie de poids inférieur de l'architecture d'addition, un deuxième groupe d'étages étant agencé pour ajouter des entrées de retenue provenant d'une partie de poids inférieur de l'architecture d'addition à des résultats provenant d'étages précédents, les étages dans les deux groupes fournissant des sorties de retenue à une partie de poids supérieur de l'architecture d'addition ; et des moyens connectés entre les premier et deuxième groupes d'étages pour extraire le résultat d'addition du premier étage en tant que produit de multiplication polynomiale, le produit de multiplication naturelle étant extrait à la

fin du deuxième groupe d'étages.

Avantageusement, l'architecture d'addition comprendra des étages en cascade de compteurs parallèles, avec au moins un compteur dans chaque colonne de produits partiels du même poids, et dans laquelle les moyens pour extraire comprennent des lignes de bit connectées au bit le moins significatif, représentant des coefficients de produits polynomiaux, à partir de chaque premier compteur dans la cascade.

Avantageusement, l'architecture d'addition comprendra un ensemble d'additionneurs complets agencés pour additionner les produits partiels et les retenues, chaque additionneur complet recevant trois entrées de poids identique et fournissant une sortie de somme du même poids et une sortie de retenue de poids supérieur suivant, un premier groupe d'additionneurs ne recevant aucun terme de retenue en tant qu'entrée, le premier groupe d'additionneurs étant agencé pour réduire des produits partiels d'un poids donné à un terme de somme, les moyens pour extraire comprenant des lignes de bit connectées aux termes de somme représentant des coefficients de produits polynomiaux, le deuxième groupe d'additionneurs recevant des entrées de retenue et des termes de somme d'un poids donné et étant agencé pour réduire les entrées de retenue et les termes de somme à des bits de produits naturels.

De préférence, le premier groupe d'additionneurs comprendra au moins une porte OU Exclusif réduisant une paire de termes à un.

De la même manière, l'architecture d'addition pourra comprendre également au moins un demi-additionneur connecté au premier groupe d'additionneurs pour réduire

une paire de termes à un.

Par ailleurs, l'ensemble de portes ET recevra des bits d'opérande et fournit des produits partiels pour plusieurs multiplications, et l'architecture d'addition additionne les produits partiels du même poids provenant des plusieurs multiplications pour fournir à la fois des résultats de multiplications polynomiale et naturelle de la forme (SUM[A_i * B_i]), où les A_i et B_i sont les opérandes et des opérandes B_i peuvent être des constantes d'un mot.

En outre, l'architecture d'addition ajoutera aux produits partiels, des bits correspondants de poids identique d'au moins un terme d'accumulation ou constant afin d'obtenir à la fois des résultats de multiplications polynomiale et naturelle de la forme (SUM[A_i * B_i] + SUM[C_i]), où C_i, ... sont les termes d'accumulation ou constants.

La présente invention se rapporte également à un procédé de multiplication de deux opérandes de n bits pour obtenir à la fois un produit de multiplication polynomiale avec des coefficients GF(2) et un produit de multiplication naturelle, le procédé comprenant :

- la génération d'un ensemble complet de produits partiels à partir de bits d'opérande, chaque produit partiel étant caractérisé par une importance ou un « poids » binaire égal à la somme des poids des bits d'opérande à partir desquels ce produit partiel a été généré ;
- l'addition des produits partiels du même poids dans des étages d'addition multiples, un premier groupe d'étages additionnant les produits partiels sans utiliser de résultats de retenue de même poids provenant

d'additions de poids inférieur, chaque addition générant une retenue de poids supérieur suivant, un deuxième groupe d'étages additionnant des résultats de somme provenant du premier groupe d'étages avec des termes de retenue du même poids ; et

- l'extraction de coefficients de produits polynomiaux des résultats de somme obtenus du premier groupe d'étages d'addition et l'extraction de bits de produits naturels des résultats de somme obtenus du deuxième groupe d'étages d'addition.

Avantageusement, l'addition des produits partiels du même poids comprendra le comptage du nombre de produits partiels qui ont une valeur binaire 1 pour fournir une valeur de comptage ayant un bit moins significatif du même poids que les produits partiels comptés et un ou plusieurs bits plus significatifs de poids relativement supérieur, la répétition ensuite des étapes de comptage dans une cascade d'étages de comptage en utilisant les bits des valeurs de comptage obtenues de l'étage précédent jusqu'à ce qu'un maximum de deux bits de chaque poids subsistent, l'exécution ensuite d'une opération d'addition finale qui s'effectue sur les paires de bits restants afin d'obtenir le produit de multiplication naturelle ; et dans lequel l'extraction des coefficients de produits polynomiaux comprend l'extraction des bits les moins significatifs obtenus de la première étape de comptage.

De préférence, l'addition des produits partiels du même poids sera effectuée uniquement avec des circuits d'additionneurs complets, chacun ayant trois entrées d'opérande, une sortie de somme et une sortie de retenue. Par ailleurs, l'addition des produits partiels comprendra

l'utilisation d'au moins un circuit de demi-additionneur dans le premier groupe d'étages.

En outre, l'extraction des coefficients de produits polynomiaux pourra comprendre l'application d'au moins une opération OU Exclusif dans le premier groupe d'étages.

Avantageusement, la génération de produits partiels à partir de bits d'opérande sera effectuée pour plusieurs opérations de multiplication, et dans lequel l'addition des produits partiels pour obtenir des résultats à la fois pour des coefficients de produits polynomiaux et pour des bits de produits naturels est également effectuée pour les plusieurs opérations de multiplication, moyennant quoi les résultats ont la forme SUM[A_i * B_i], où A_i et B_i sont les opérandes et des opérandes B_i peuvent être des constantes d'un mot.

Par ailleurs, l'étape d'addition pourra comprendre, en outre, l'addition, aux produits partiels, de bits correspondants de poids identique d'au moins un terme d'accumulation ou constant pour obtenir des résultats à la fois pour des coefficients de produits polynomiaux et pour des bits de produits naturels ayant la forme (SUM[A_i * B_i] + SUM[C_i]), où C_i, ..., sont les termes d'accumulation ou constants.

Un mode d'exécution de l'invention sera décrit ci-après, à titre d'exemple non limitatif, avec référence aux figures annexées dans lesquelles :

La figure 1 est une vue plane schématique d'une architecture de multiplicateurs naturels parallèles de l'art antérieur selon Dadda.

La figure 2 est une vue plane schématique d'une

version modifiée de la figure 1 qui a été pourvue de lignes de bit qui extraient des bits de produit binaire de compteurs internes en tant que sortie séparée en plus du produit naturel.

La figure 3 est un schéma de principe d'architectures de multiplicateurs générales selon la présente invention.

La figure 4 est une partie de circuit schématique pour un générateur de produit partiel utilisé dans n'importe quel circuit de multiplicateur.

La figure 5 est un schéma de circuit d'une tranche d'additionneur sans propagation de retenue de l'art antérieur avec huit entrées de produit partiel de poids identique.

La figure 6 est un schéma de circuit d'un mode de réalisation de la présente invention d'une tranche d'additionneur sans propagation de retenue avec une porte OU Exclusif supplémentaire pour l'extraction du bit de produit polynomial.

La figure 7 est un schéma de circuit d'un autre mode de réalisation d'une tranche d'additionneur sans propagation de retenue selon la présente invention, utilisant un demi-additionneur et une extraction de ligne de bit du bit de produit polynomial.

Les figures 8A à 8G montrent des schémas de circuit pour des tranches similaires à la figure 6 avec une à sept entrées de produit partiel, avec une porte OU Exclusif supplémentaire pour chaque tranche ayant un nombre pair d'entrées de produit partiel.

La figure 9 est un schéma de principe pour deux poids adjacents k et k + 1 montrant une structure d'additionneurs capable de gérer également la

multiplication d'entiers négatifs.

En faisant référence à la figure 2, une variante de l'architecture de Dadda (figure 1) reconnaît que le bit le moins significatif 13 de chaque compteur 11 dans la zone B, avec les termes de produit solo 15 des première et dernière colonnes, correspond aux bits de produit polynomial pour des polynômes avec des coefficients dans GF(2). Ces bits les moins significatifs 13 du compteur sont extraits par l'intermédiaire de lignes de bit 17 et délivrés en tant que sortie de produit polynomial, séparés du produit naturel obtenu dans la zone R et en plus de celui-ci. Bien que ces bits de produit polynomial pourraient être présents en tant qu'états internes de certains circuits de multiplication naturelle, à la connaissance de l'inventeur, ils n'ont pas été extraits séparément pour réaliser un multiplicateur fournissant à la fois des produits polynomiaux et naturels.

La reconnaissance qu'une somme de produits dans GF(2) peut être présente et disponible pour une extraction dans des architectures de multiplicateurs naturels, suggère que des multiplicateurs pourraient être conçus spécifiquement pour fournir à la fois des produits polynomiaux et naturels, à savoir par un groupement approprié de l'architecture d'addition de produits partiels. Cela est possible grâce à un réagencement du produit naturel C en deux parties, lequel comprend le produit polynomial D et les termes supplémentaires E qui représentent une suite de l'opération de sommation :

$$C = SUM_{i,j}\ (a_i,\ b_j.2^{i+j})$$
$$= SUM_k\ ((SUM_{i+j-k}\ (AND(a_i,\ b_j))).2^k)$$

$$= SUM_k\ (XOR_{j-k-i}\ [AND_{i+j-k}(a_i,\ b_j)/2^k] +$$
$$SUM_k\ (e_k.2^k)$$
$$= D + SUM_k\ (e_k.2^k)$$

où les e_k sont tous les termes de retenue de poids k obtenus à partir des additions de poids inférieur suivant k - 1. Ces termes d'addition sont sans rapport avec le produit de multiplication polynomiale D, mais poursuivent simplement l'addition de la multiplication naturelle pour obtenir le produit naturel C. N'importe quelle architecture de multiplication qui sépare les additions de retenues en un deuxième groupe d'étages fait en sorte de réaliser la multiplication naturelle et de fournir également le résultat de multiplication polynomiale D provenant d'un premier groupe d'étages d'addition qui utilise uniquement des produits partiels et aucune retenue.

La figure 3 représente de manière schématique cette séparation en deux groupes 23 et 29 d'additionneurs et l'extraction 27 et 33 des différents produits provenant des deux groupes. En particulier, les bits d'opérande a_i et b_j, où i et j sont tous deux dans la plage de 0 à n - 1, sont reçus par un ensemble 21 ou des portes ET (symbolisées par un x encerclé) afin de produire un ensemble complet de termes de produit partiel $p_{i,j}$, caractérisés chacun par un degré ou un poids polynomial w_k, où k = i + j et se trouve dans la plage de 0 à 2n - 2. Les produits partiels sont ensuite reçus par un premier groupe 23 de structures d'addition (symbolisées par des + encerclés) qui sont séparées pour chaque degré ou poids polynomial (symbolisé par les traits pleins 25). Ces structures d'addition réduisent les termes de produit

$p_{i,j}$ à un ensemble de termes de somme s_k et un ensemble de termes de retenue e_{k+1}. Pour un poids donné k, il peut y avoir plusieurs lignes de termes de retenue e_{k+1}. Étant donné que l'addition de premier étage a été effectuée pour chaque degré ou poids séparément sans appliquer la moindre retenue résultant de l'une quelconque des opérations d'addition, les termes de somme s_k représentent les termes de produit polynomial et sont extraits le long des lignes de bit 27 afin de former les coefficients de produit polynomial d_k, où k se trouve toujours dans la plage de 0 à 2n - 2. Dans cette extraction, n'importe quelles paires de somme de termes de même degré polynomial peuvent être soumises à une opération OU Exclusif afin de produire un bit de produit unique pour chaque degré. Les termes de somme s_k et les termes de retenue e_{k+1} sont appliqués à un deuxième groupe 29 de structures d'addition (symbolisées de nouveau par des + encerclés). Mais ici, n'importe quels termes de retenue (symbolisés par des diagonales 31 croisant des limites de poids en pointillé) sont inclus dans les entrées des structures d'addition. Les additions du deuxième étage, réalisées éventuellement par un ensemble d'additionneurs à propagation de retenue, d'additionneurs sans propagation de retenue ou de réducteurs 4 vers 2, réduisent à un ensemble de sorties 33 qui représentent les bits de produits naturels c_k, où, du fait de l'incorporation des termes de retenue, k se trouve maintenant dans la plage de 0 à 2n - 1. Ainsi, les deux produits de multiplication polynomiale et naturelle sont obtenus et sortis du circuit. Cela n'est généralement pas beaucoup plus lent qu'une architecture de multiplication naturelle rapide classique. En fait, à part le fait que

certaines structures optimisées sont exclues par la spécification précisant que les additions de termes de retenue doivent être différées jusqu'au deuxième groupe de structures d'addition, l'architecture est autrement aussi rapide que d'autres multiplicateurs de construction similaire. Quant à la taille, le matériel supplémentaire nécessaire pour extraire le produit binaire est négligeable, par exemple quelques lignes de bit supplémentaires ou quelques portes OU Exclusif supplémentaires. Notez que, bien que ce mode de réalisation illustré multiplie deux opérandes de n bits, l'invention fonctionne aussi bien dans des cas non symétriques avec des opérandes de différentes tailles (multiplication m x n et multiplication-accumulation, y compris les opérations de multiplication-accumulation 1 x n + n).

Sur la figure 4, les éléments de circuit de génération de produit partiel sont vus comme étant composés de porte ET. Chaque porte ET 41 reçoit deux entrées correspondant aux bits d'opérande a_i et b_j. La porte ET délivre le produit partiel $p_{i,j}$ pour cette paire de bits d'opérande, qui relie un ensemble d'autres produits partiels de degré ou de poids polynomial identique k (= i + k). D'autres éléments de circuit de génération de produit partiel pourraient être utilisés. Par exemple, il pourrait s'agir de portes NON ET, si une logique à un certain point rétablit ensuite la polarité correcte. Cette étape de rétablissement peut être effectuée après l'ensemble d'additionneurs étant donné que, si nous avons carryOut, sum = a + b + c, alors nous avons également non(carryOut), non(sum) = non(a) + non(b) + non(c). De même, nous pourrions utiliser des

portes OU ou des portes NON OU conformément à des conventions de polarité ; ou des additionneurs qui fonctionnent avec des polarités inversées au niveau des entrées ou des sorties.

En faisant référence aux figures 5 à 7, les termes de produit partiel du même degré ou poids sont additionnés dans un circuit additionneur, constitué, par exemple, largement d'additionneurs complets. Les additionneurs complets sont des éléments de circuit bien connus qui additionnent trois entrées pour générer une somme et une retenue. Les entrées peuvent être des produits partiels, des termes de somme du même degré ou poids provenant d'autres additionneurs dans la tranche, ou des termes de retenue reçus de la tranche d'additionneurs de poids inférieur suivant. Tous les termes de retenue générés par les additionneurs sont de poids supérieur suivant et sont délivrés (pour une multiplication naturelle) à une tranche adjacente. Les éléments de circuit d'additionneur sur les figures 5 à 7 ont tous huit entrées de produit partiel $p_{i,j}$, avec i et j compris entre 0 et 7 et le poids i + k = 7. Chaque circuit a également 6 retenues d'entrée, 6 retenues de sortie et 2 termes de sortie de produit naturel. Deux termes de sortie correspondent à un cas type, où, à la fin, un additionneur rapide (à anticipation de retenue, à sélection de retenue ou autre) recueillera les deux lignes de sortie dans chacune des différentes tranches afin de calculer le produit final. Une autre architecture peut générer une seule ou plus de deux lignes de sortie du poids envisagé. Les figures 6 et 7 fournissent également un terme de sortie de produit polynomial. D'autres tranches d'additionneur de poids différent

peuvent avoir un nombre différent d'entrées de produit partiel. Sur les figures 5 à 7, les entrées de retenue et les sorties de retenue sont alignées comme si les tranches étaient identiques. Ceci est proche de la situation réelle, bien qu'il puisse y avoir un terme de retenue d'entrée en moins (ou en plus) lorsque le nombre d'entrées de produit partiel augmente (ou diminue) avec l'augmentation du poids. Avec l'augmentation du poids, le nombre d'entrées de produit partiel augmente dans la moitié la moins significative de la multiplication et diminue dans la moitié la plus significative de la multiplication.

Sur la figure 5, une tranche d'additionneur sans propagation de retenue de l'art antérieur additionne avec des additionneurs complets 51 à 53 autant de produits partiels que possible sans recevoir d'entrées de retenue (ici, 7 parmi les 8 entrées de produit partiel). Même ainsi, un huitième terme de produit partiel est ajouté aux entrées de terme de retenue c, dans un additionneur complet 54. Les additions suivantes par des additionneurs complets 55 à 57 additionnent les sommes provenant des additionneurs complets 53 et 54 et additionnent également les entrées de retenue c_7. Les termes de retenue c_8 de poids supérieur suivant sont délivrés à une tranche adjacente. La tranche d'additionneur délivre une sortie de somme, qui peut être ajoutée à n'importe quel terme d'entrée de retenue restant dans un étage d'additionneurs à propagation de retenue suivant. L'arrangement effectue une réduction de 8 à 2 dans des retards de 4 additionneurs. Étant donné que la figure 5 est une tranche d'additionneurs pour un multiplicateur naturel uniquement, le produit binaire pour une multiplication à

domaine fini n'est pas disponible.

L'agencement sans propagation de retenue de la figure 6 est sensiblement identique à celui de la figure 5, excepté qu'un bit de produit polynomial est créé par une addition à OU Exclusif. Sur la figure 6, un agencement d'additionneurs sans propagation de retenue modifié a de nouveau 8 entrées de produit partiel de poids identique (i + j = k = 7). De nouveau, 7 des termes sont additionnés par des additionneurs complets 61 à 63. La somme résultante, ainsi que la huitième entrée de produit partiel, sont extraites sur les lignes 67 et 68 et appliquée à une porte OU Exclusif 69 afin d'obtenir le terme polynomial $PMUL_7$ de degré 7. La somme provenant de l'additionneur 63, la huitième entrée de produit partiel, et les entrées de retenue c_7 sont également additionnées en utilisant des additionneurs complets 64 à 66 afin d'obtenir un terme de somme et jusqu'à un terme d'entrée de retenue restant pour une addition subséquente par un additionneur à propagation de retenue afin d'obtenir le bit de multiplication naturelle correspondant. Ainsi, le circuit modifié effectue les mêmes additions que sur la figure 6, mais avec une porte OU Exclusif supplémentaire qui extrait le terme de produit polynomial Le retard des additionneurs n'est pas très différent de celui du circuit de la figure 5.

Sur la figure 7, une modification différente de l'agencement sans propagation de retenue de la figure 5 introduit un circuit de demi-additionneur. Les demi-additionneurs sont des circuits bien connus qui ne reçoivent que deux entrées et génèrent des sorties de somme et de retenue. L'utilisation d'un demi-additionneur permet l'addition des huit entrées de produit partiel de

la figure 7. Trois des entrées sont traitées par un premier additionneur complet 71, trois autres entrées sont traitées par un deuxième additionneur complet 72 et les deux entrées finales sont traitées par le demi-additionneur 73. Les sorties de somme des trois additionneurs 71 à 73 sont additionnées par un additionneur complet 74 afin d'obtenir le terme de produit polynomial $PMUL_7$. Les additions de la sortie de somme de l'additionneur 74 aux entrées de retenue c_7 sont traitées par des additionneurs complets 75 à 77. De nouveau, il n'y a aucune pénalité significative dans les retards des additionneurs. Le mode de réalisation de la figure 7 nécessite un demi-additionneur supplémentaire et un terme de retenue supplémentaire, par rapport à la figure 5. (Le terme de retenue supplémentaire est dû au fait qu'un additionneur complet n'utilise jamais la combinaison totale des sorties de somme et de retenue. En fait, le cas (retenue, somme) = (1, 1) n'est pas possible.

En faisant référence aux figures 8a à 8g, le mode de réalisation de la figure 6 est étendu afin de montrer un certain nombre d'agencements pour différents nombres d'entrées de produit partiel. La porte OU Exclusif supplémentaire n'est nécessaire que lorsqu'il y a un nombre pair d'entrées de produit partiel. Pour un nombre impair, les additionneurs réduisent à un terme de somme unique avant d'ajouter les retenues. Ainsi, pour un nombre impair d'entrées de produit partiel, la tranche ne nécessite qu'une ligne de bit supplémentaire pour extraire le terme de bit de produit polynomial $PMUL_i$. Excepté pour le cas à deux entrées, le côté ascendant de l'architecture d'addition (degrés ou poids 0 à n - 1) a

une entrée de retenue de moins et ainsi une seule entrée de somme vers l'étage d'additionneurs à propagation de retenue qui suit. Pour des degrés ou des poids n à 2n - 2, il y aura à la fois une entrée de somme et de retenue délivrée par les tranches à l'étage d'additionneurs à propagation de retenue. Pour des multiplicateurs plus grands, par exemple 32 x 32, la séquence d'additionneurs complets et de portes OU Exclusif continue de s'étendre dans la moitié la moins significative de la multiplication, se réduit ensuite dans la moitié la plus significative de la multiplication, avec des entrées de produit partiel de numéro pair nécessitant que la tranche ait une porte OU Exclusif pour délivrer le terme de produit polynomial. Une progression similaire se produit pour l'utilisation d'un demi-additionneur (nécessaire pour un nombre pair d'entrées de produit partiel).

Les figures 6, 7 et 8A à 8G représentent des mises en oeuvre exemplaires de modes de réalisation préférés selon la présente invention. Cependant, d'autres mises en oeuvre de l'invention sont également possibles. Par exemple, bien que les mises en oeuvre montrées ci-dessus utilisent un OU Exclusif ou un demi-additionneur pour des cas ayant un nombre pair d'entrées de produit partiel, d'autres mises en oeuvre possible pourraient choisir d'avoir plusieurs OU Exclusifs ou demi-additionneurs ou pourraient également utiliser un OU Exclusif ou un demi-additionneur dans les cas avec un nombre impair d'entrées de produit partiel. Bien que ces variantes seraient loin d'être optimales en termes de nombre de portes, elles pourraient être choisies pour faciliter l'agencement, le mappage vers un dispositif FPGA ou pour une autre raison quelconque. Par ailleurs, l'emplacement des OU Exclusifs

ou des demi-additionneurs dans l'arborescence d'additionneurs peut varier par rapport à celui qui est montré. En outre, bien que les configurations des figures 6 et 7 aient un nombre identique d'entrées de retenue et de sorties de retenue, les figures 8A à 8G illustrent que cela ne doit pas nécessairement être toujours le cas. Et bien que les mises en oeuvre ci-dessus soient réalisées avec des additionneurs complets et des demi-additionneurs ou des portes OU Exclusif, d'autres blocs de construction tels que des réducteurs 4 à 2 peuvent être utilisés.

Le cas de la multiplication-addition, C = A.D + Z est utilisé à la fois pour une multiplication-accumulation C := A.B + C ou C = A.B + F.G + K.L et pour calculer le produit de multiplicandes, dont l'un ou les deux est plus grand que le matériel de multiplicateur, par exemple une multiplication sur 160 bits utilisant un circuit de multiplication de 32 bits. Dans ces cas, un nombre à ajouter peut être traité comme s'il consistait en un ensemble supplémentaire de produits partiels à ajouter. Pour le cas d'une multiplication-addition naturelle, toutes les retenues sont incluses dans le résultat. Pour une multiplication-addition polynomiale avec des coefficients dans GF(2), toutes les retenues ne croisent pas les limites des degrés polynomiaux et sont ainsi ignorées.

Pour une multiplication naturelle, la gestion d'une grandeur supérieure peut être réduite à une série d'opérations de multiplication et d'addition. Pour une grandeur de mot matérielle de L bits et une grandeur d'opérande de M mots, c'est-à-dire que P = M.L bits, et des opérandes de codage d'une manière naturelle, $A = SUM_1(A_1 - 2^i)$, pour un indice i compris entre 0 et P - 1,

nous pouvons, en variante, représenter l'opérande par des mots, $A = SUM_j({}_jA.w^j)$, où $w = 2^L$, un indice à gauche est utilisé pour l'indexage de mots, comme dans le mot ${}_jA$, l'indice j variant de 0 à M - 1 et le bit ${}_jA_i = A_{j.L+1}$. Ainsi, le produit des deux opérandes A et B est :

$$A.B = SUM_k\ (SUM_{i+j-k}({}_iA.{}_jB).w^k).$$

La quantité $SUM_{i+j-k}({}_iA.{}_jB)$ est une somme de produits du même poids et, par conséquent, la multiplication de grande largeur est effectuée par une série de multiplications $({}_iA.{}_jB)$ et d'additions (SUM_k). En général, le résultat de chaque opération de multiplication est codé sur 2L bits pour la multiplication, plus quelques bits supplémentaires alors que les additions sont effectuées. Ce qui est au-delà de w, c'est-à-dire les bits de résultat avec des poids supérieurs ou égaux à L, devrait être injecté par la suite lorsque les k + 1 indices sont traités.

Pour une multiplication polynomiale avec des coefficients dans GF(2), la notation utilisée ci-dessus pour une multiplication naturelle est de nouveau utilisée, mais le symbole * est utilisé pour représenter une multiplication polynomiale $A - SUM_i(A_i.x^i)$, pour un indice i compris entre 0 et p - 1. Ceci est traité par un matériel de L bits tel que $A = SUM_j({}_jA.w^j)$, où ${}_jA$ sont des polynômes de L bits, avec un indice j compris entre 0 et M - 1 et $w = x^L$. Les polynômes ${}_jA$ sont définis par :

$${}_jA = SUM_i(A_{j.L+1}.x^i)$$

avec i compris entre 0 et L - 1. Le produit polynomial

est alors :

$$A * B = SUM_k(XOR_{i+j-k}({}_iA * {}_jB).w^k),$$

avec k entre 0 et 2M - 2, où la quantité $x_k = XOR_{i+j-k}({}_iA * {}_jB)$ est une somme polynomiale de produits partiels polynomiaux du même degré, tous les coefficients ayant des valeurs dans GF(2), c'est-à-dire sans faire référence aux retenues. Les produits polynomiaux élémentaires sont codés exactement sur 2L - 2 bits et aucun bit supplémentaire n'est ajouté étant donné que l'addition polynomial ne mène pas à une augmentation de degré. Ce qui est au-delà de W, c'est-à-dire la partie de résultat de degré supérieur ou égal à L, devrait être injecté par la suite lorsque les k + 1 indices sont traités, par une addition polynomiale (c'est-à-dire, un OU Exclusif) des polynômes.

Une adaptation supplémentaire possible consiste à intégrer la multiplication et l'addition dans des opérations de multiplication-accumulation. La plupart des gens pensent habituellement qu'une opération de multiplication-accumulation, C = A.B + C est tout d'abord une multiplication avec un résultat intermédiaire A.B et ensuite une addition pour obtenir le résultat final. Cependant, cela n'est pas nécessaire, et un matériel de multiplication-addition peut être réalisé pour intégrer la multiplication et l'addition, avec à la fois les produits partiels et les bits ou coefficients d'accumulation devant être additionnés. C'est-à-dire, former les produits partiels $A_i.B_j$, les additionner ensuite aux bits d'accumulation C_k du poids approprié. Il est simplement nécessaire de prévoir un ensemble

d'additionneurs qui peut également recevoir les bits C_k provenant d'un bus C supplémentaire. Dans le cas d'une multiplication-addition de polynôme avec des coefficients dans GF(2), on obtient les bits de produit partiel et les bits d'accumulation d'une manière non différenciée aux entrées de l'ensemble d'additionneurs et on effectue un OU Exclusif entre plusieurs éléments de même poids sans impliquer le moindre bit de retenue :

$$D = A * B + C - SUM_k(XOR_{i+j=k}(AND(A_i, B_j), c_k).2^k)$$

Pour une multiplication-addition de polynômes avec des coefficients dans GF(2), on doit placer, au niveau de l'entrée d'une tranche de degré k, tous les produits partiels nécessaires, et le coefficient de polynôme de degré k provenant de C à ajouter, et élaborer les tranches de l'ensemble d'addition de sorte que les sommes de ces entrées soient disponibles en tant que sortie polynomiale de cette tranche :

$$D = A * B + C - SUM_k(SUM_{i+j=k}({}_iA.{}_jB), {}_kC).w^k),$$

où les indices font référence ici aux poids des coefficients de polynôme de N bits.

Une intégration de l'opération de multiplication-addition peut également être généralisée davantage afin d'inclure, par exemple, A1 * B1 + A2 * B2 + C, où A1 * B1 est la multiplication actuelle à effectuer, A2 * B2 est le travail constant de Montgomery (ou Barrett) pour une extraction modulaire, et C permet une accumulation ou une extension à des grands nombres. Par ailleurs, bien que la description ci-dessus ait été principalement dédiée à la

partie de multiplication polynomiale d'une opération à domaine fini, des opérations de réduction polynomiale dans un domaine fini peuvent également suivre la multiplication ou même être intégrées dans une opération de multiplication-réduction à domaine fini combinée. Les opérations possibles que le circuit multiplicateur pourrait effectuer pourraient comprendre les opérations de multiplication de N x M mots dans le cas où M = 1, c'est-à-dire des opérations de multiplication de N x 1 mots. Par exemple, une multiplication par une constante b d'un mot, éventuellement avec une étape d'accumulation suivante (A * b ou A * b + C), pourrait être effectuée pour une extension à un multiple de plus grande taille. De même, le cas de multiplication et d'accumulation double indiqué ci-dessus pourrait être appliqué à des multiplicandes d'un mot b1 et b2 (A1b1 + A2b2 + C), dans une multiplication naturelle ou polynomiale, et dans ce dernier cas avec ou sans réduction modulaire subséquente (Barrett, Montgomery ou d'autres types). Deux unités de multiplicateurs parallèles ou plus, l'une d'elles au moins pouvant être sélectionnée pour une sortie de produit naturel ou polynomial selon la présente invention, peuvent être prévues pour effectuer les opérations plus générales.

Jusqu'ici, nous avons décrit un multiplicateur capable de traiter des polynômes ou des entiers positifs. L'invention peut être adaptée pour traiter des entiers négatifs également. Par exemple, une notation en complément à deux peut être utilisée pour représenter à la fois des nombres positifs et négatifs :

$$A = -a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \ldots + a_0 \cdot 2^0,$$

où a_n est le « bit de signe ». Si $a_n = 1$, alors A est négatif ; si $a_n = 0$, alors A est positif ou égal à zéro. Avec (n + 1) bits, les valeurs de A peuvent être comprises entre -2^n et $2^n - 1$. Pour un complément à deux, une multiplication naturelle est :

$$A \cdot B = a_n \cdot b_n \cdot 2^{2n} - a_n(b_{n-1} \cdot 2^{2n-1} + \ldots + b_0 \cdot 2^n) - b_n(a_{n-1} \cdot 2^{2n-1} + \ldots + a_0 \cdot 2^n) + \text{sum}_{0 \le i,j < n}(a_i \cdot b_j \cdot 2^{i+j})$$

$$= a_n \cdot b_n \cdot 2^{2n} - 2^{2n+1} + 2^{n+1} + [\text{not } (a_n \cdot b_{n-1}) \cdot 2^{2n-1} + \ldots + \text{not } (a_n \cdot b_0) \cdot 2^n] [\text{not } (b_n \cdot a_{n-1}) \cdot 2^{2n-1} + \ldots + \text{not } (b_n \cdot a_0) \cdot 2^n] + \text{sum}_{0 \le i,j < n}(a_i \cdot b_j \cdot 2^{i+j}).$$

Le dernier terme, $\text{sum}_{0 \le i,j < n}(a_i \cdot b_j \cdot 2^{i+j})$, est identique à celui d'une multiplication positive sur n * m bits. Dans cette partie, nous pouvons facilement extraire la multiplication polynomiale, comme montré précédemment dans ce document, tant que l'architecture du multiplicateur est organisée de sorte qu'aucune interférence n'existe avec le reste des termes dans le calcul.

Tous ces autres termes, c'est-à-dire, les produits partiels inversés de poids élevé et une constante 2^{n+1}, doivent être ajoutés afin d'obtenir le résultat de la multiplication naturelle. Cependant, parce qu'une addition est associative et commutative, le résultat ne changera pas si cette addition est effectuée ultérieurement dans le traitement. Afin que l'addition de ces termes soit effectuée à une vitesse et un coût

optimaux, il est préférable d'injecter ces termes à additionner aussitôt que l'extraction polynomiale est achevée.

La figure 9 montre un schéma de principe d'une partie de la structure d'additionneurs de l'architecture de multiplicateurs pour mettre en oeuvre la multiplication à complément à deux mentionnée ci-dessus. Sur la figure 9, des étages d'additionneurs 91_k et 91_{k-1} pour deux poids adjacents k et (k + 1) sont montrés comme comprenant des premiers étages d'addition 95_k et 95_{k+1}, respectivement, qui additionnent des produits partiels positifs, 93_k et 93_{k+1} de poids particulier (k ou k + 1) sans utiliser le moindre terme de retenue afin d'obtenir les bits de produit polynomial de ce même poids sur les sorties OU Exclusif des étages d'additionneurs, 97_k et 97_{k+1}. Ces bits polynomiaux peuvent être extraits comme dans les modes de réalisation antérieurs afin de produire un produit polynomial D'autres étages d'addition, 99_k et 99_{k+1}, reçoivent également les bits polynomiaux, 97_k et 97_{k+1}, ainsi que des termes de retenue, 101_k et 101_{k+1}, délivrés par les premiers étages d'addition de poids inférieur suivant. Afin de traiter à la fois des entiers positifs et négatifs, eiuuggtr0.g, sous forme de complément à deux, les produits partiels inversés, 2^{n+1} bits (et d'autres termes dans l'équation décrite juste ci-dessus) sont appliqués sur les lignes de bit, 103_k et 103_{k+1}, de poids correspondant aux autres étages d'addition 99_k et 99_{k+1}. C'est-à-dire que 2^{n+1} est délivré uniquement à l'étage d'additionneur 99_{n+1} de poids n + 1. Les autres étages d'addition, 99_k et 99_{k+1}, délivrent les bits de produits naturels 105_k et 105_{k+1}.

Un tel multiplicateur est capable de prendre en

charge :

(1) une multiplication positive n * n, par une remise à zéro des bits de signe ;

(2) une multiplication en complément à deux (n + 1) * (n + 1) ;

(3) une multiplication en complément à deux n * n, par une extension de signe au (n + 1) bit ; et

(4) une multiplication polynomiale n * n, par une extraction de bit de produit polynomial, comme expliqué.

Le même procédé est applicable à une multiplication m * n ou à une multiplication-accumulation par (a) une extension de signe afin d'avoir uniquement une représentation positive pour des lignes d'entrée vers une multiplication (-accumulation) polynomiale ; (b) un traitement séparé des lignes qui concernent une multiplication (-accumulation) polynomiale, c'est-à-dire des produits partiels, un OU Exclusif par des additionneurs, des demi-additionneurs ou de simples OU Exclusifs ; (c) une extraction du résultat polynomial ; et (d) une consolidation de l'addition d'ensemble uniquement après que le résultat polynomial ait été extrait.

REVENDICATIONS

1. Architecture matérielle de multiplicateurs parallèles qui délivre à la fois un produit de multiplication polynomiale avec des coefficients dans GF(2) et un produit de multiplication naturelle, l'architecture de multiplicateurs comprenant :

- un ensemble de portes ET avec des entrées connectées à des bits d'opérande et avec des sorties délivrant un ensemble complet de produits partiels des bits d'opérande, chaque produit partiel étant caractérisé par une importance ou un « poids » de bit ;
- une architecture d'addition agencée pour additionner des produits partiels du même poids, l'architecture d'addition étant réalisée par des étages multiples, un premier groupe d'étages étant agencé pour additionner des produits partiels sans recevoir la moindre entrée de retenue d'une partie de poids inférieur de l'architecture d'addition, un deuxième groupe d'étages étant agencé pour ajouter des entrées de retenue provenant d'une partie de poids inférieur de l'architecture d'addition à des résultats provenant d'étages précédents, les étages dans les deux groupes fournissant des sorties de retenue à une partie de poids supérieur de l'architecture d'addition ; et
- des moyens connectés entre les premier et deuxième groupes d'étages pour extraire le résultat d'addition du premier étage en tant que produit de multiplication polynomiale, le produit de multiplication naturelle étant extrait à la fin du deuxième groupe d'étages.

2. Architecture de multiplicateurs selon la revendication

1, caractérisée en ce que l'architecture d'addition comprend des étages en cascade de compteurs parallèles, avec au moins un compteur dans chaque colonne de produits partiels du même poids, et dans laquelle les moyens pour extraire comprennent des lignes de bit connectées au bit le moins significatif, représentant des coefficients de produits polynomiaux, à partir de chaque premier compteur dans la cascade.

3. Architecture de multiplicateurs selon la revendication 1, caractérisée en ce que l'architecture d'addition comprend un ensemble d'additionneurs complets agencés pour additionner les produits partiels et les retenues, chaque additionneur complet recevant trois entrées de poids identique et fournissant une sortie de somme du même poids et une sortie de retenue de poids supérieur suivant, un premier groupe d'additionneurs ne recevant aucun terme de retenue en tant qu'entrée, le premier groupe d'additionneurs étant agencé pour réduire des produits partiels d'un poids donné à un terme de somme, les moyens pour extraire comprenant des lignes de bit connectées aux termes de somme représentant des coefficients de produits polynomiaux, le deuxième groupe d'additionneurs recevant des entrées de retenue et des termes de somme d'un poids donné et étant agencé pour réduire les entrées de retenue et les termes de somme à des bits de produits naturels.

4. Architecture de multiplicateurs selon la revendication 3, caractérisée en ce que le premier groupe d'additionneurs comprend au moins une porte OU Exclusif réduisant une paire de termes à un.

5. Architecture de multiplicateurs selon la revendication 3, caractérisée en ce que l'architecture d'addition comprend également au moins un demi-additionneur connecté au premier groupe d'additionneurs pour réduire une paire de termes à un.

6. Architecture de multiplicateurs selon la revendication 1, caractérisée en ce que l'ensemble de portes ET reçoit des bits d'opérande et fournit des produits partiels pour plusieurs multiplications, et l'architecture d'addition additionne les produits partiels du même poids provenant des plusieurs multiplications pour fournir à la fois des résultats de multiplications polynomiale et naturelle de la forme (SUM[A_i * B_i]), où les A_i et B_i sont les opérandes et des opérandes B_i peuvent être des constantes d'un mot.

7. Architecture de multiplicateurs selon la revendication 6, caractérisée en ce que l'architecture d'addition ajoute, en outre, aux produits partiels, des bits correspondants de poids identique d'au moins un terme d'accumulation ou constant afin d'obtenir à la fois des résultats de multiplications polynomiale et naturelle de la forme (SUM[A_i * B_i] + SUM[C_i]), où C_i, ... sont les termes d'accumulation ou constants.

8. Procédé de multiplication de deux opérandes de n bits pour obtenir à la fois un produit de multiplication polynomiale avec des coefficients GF(2) et un produit de multiplication naturelle, le procédé comprenant :

- la génération d'un ensemble complet de produits

partiels à partir de bits d'opérande, chaque produit partiel étant caractérisé par une importance ou un « poids » binaire égal à la somme des poids des bits d'opérande à partir desquels ce produit partiel a été généré ;

- l'addition des produits partiels du même poids dans des étages d'addition multiples, un premier groupe d'étages additionnant les produits partiels sans utiliser de résultats de retenue de même poids provenant d'additions de poids inférieur, chaque addition générant une retenue de poids supérieur suivant, un deuxième groupe d'étages additionnant des résultats de somme provenant du premier groupe d'étages avec des termes de retenue du même poids ; et
- l'extraction de coefficients de produits polynomiaux des résultats de somme obtenus du premier groupe d'étages d'addition et l'extraction de bits de produits naturels des résultats de somme obtenus du deuxième groupe d'étages d'addition.

9. Procédé de multiplication selon la revendication 8, caractérisé en ce que l'addition des produits partiels du même poids comprend le comptage du nombre de produits partiels qui ont une valeur binaire 1 pour fournir une valeur de comptage ayant un bit moins significatif du même poids que les produits partiels comptés et un ou plusieurs bits plus significatifs de poids relativement supérieur, la répétition ensuite des étapes de comptage dans une cascade d'étages de comptage en utilisant les bits des valeurs de comptage obtenues de l'étage précédent jusqu'à ce qu'un maximum de deux bits de chaque poids subsistent, l'exécution ensuite d'une opération

d'addition finale qui s'effectue sur les paires de bits restants afin d'obtenir le produit de multiplication naturelle ; et

dans lequel l'extraction des coefficients de produits polynomiaux comprend l'extraction des bits les moins significatifs obtenus de la première étape de comptage.

10. Procédé de multiplication selon la revendication 8, caractérisé en ce que l'addition des produits partiels du même poids est effectuée uniquement avec des circuits d'additionneurs complets, chacun ayant trois entrées d'opérande, une sortie de somme et une sortie de retenue.

11. Procédé de multiplication selon la revendication 8, caractérisé en ce que l'addition des produits partiels comprend l'utilisation d'au moins un circuit de demi-additionneur dans le premier groupe d'étages.

12. Procédé de multiplication selon la revendication 8, caractérisé en ce que l'extraction des coefficients de produits polynomiaux comprend l'application d'au moins une opération OU Exclusif dans le premier groupe d'étages.

13. Procédé de multiplication selon la revendication 8, caractérisé en ce que la génération de produits partiels à partir de bits d'opérande est effectuée pour plusieurs opérations de multiplication, et dans lequel l'addition des produits partiels pour obtenir des résultats à la fois pour des coefficients de produits polynomiaux et pour des bits de produits naturels est également effectuée pour les plusieurs opérations de

multiplication, moyennant quoi les résultats ont la forme (SUM[A_i * B_i]), où A_i et B_i sont les opérandes et des opérandes B_i peuvent être des constantes d'un mot.

14. Procédé de multiplication selon la revendication 13, caractérisé en ce que l'étape d'addition comprend, en outre, l'addition, aux produits partiels, de bits correspondants de poids identique d'au moins un terme d'accumulation ou constant pour obtenir des résultats à la fois pour des coefficients de produits polynomiaux et pour des bits de produits naturels ayant la forme (SUM[A_i * B_i] + SUM[C_i]), où C_i, ..., sont les termes d'accumulation ou constants.

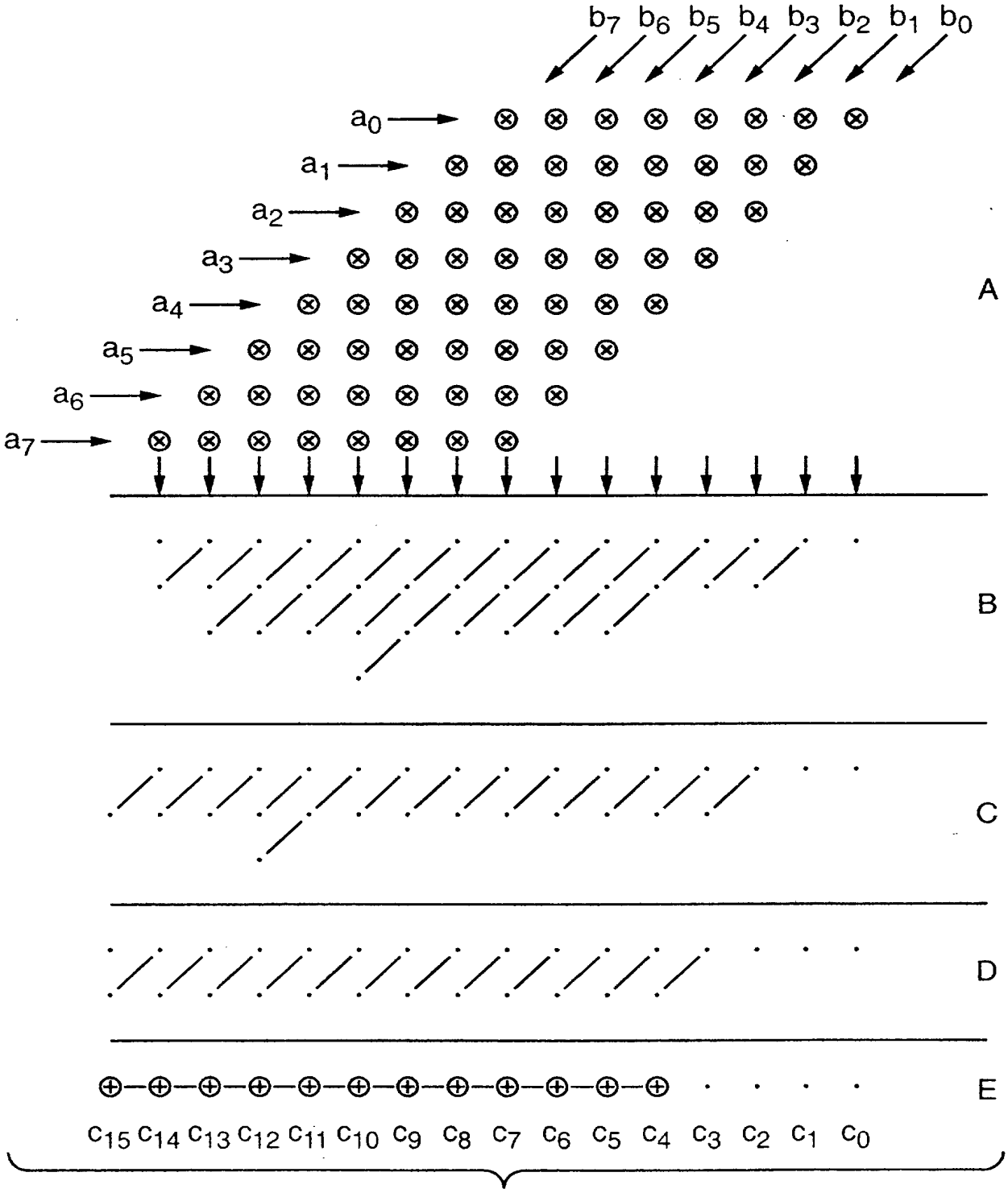
b7 b6 b5 b4 b3 b2 b1 b0
a0
a1
a2
a3
a4
a5
a6
a7
A
B
C
D
E
c15 c14 c13 c12 c11 c10 c9 c8 c7 c6 c5 c4 c3 c2 c1 c0

FIG._1

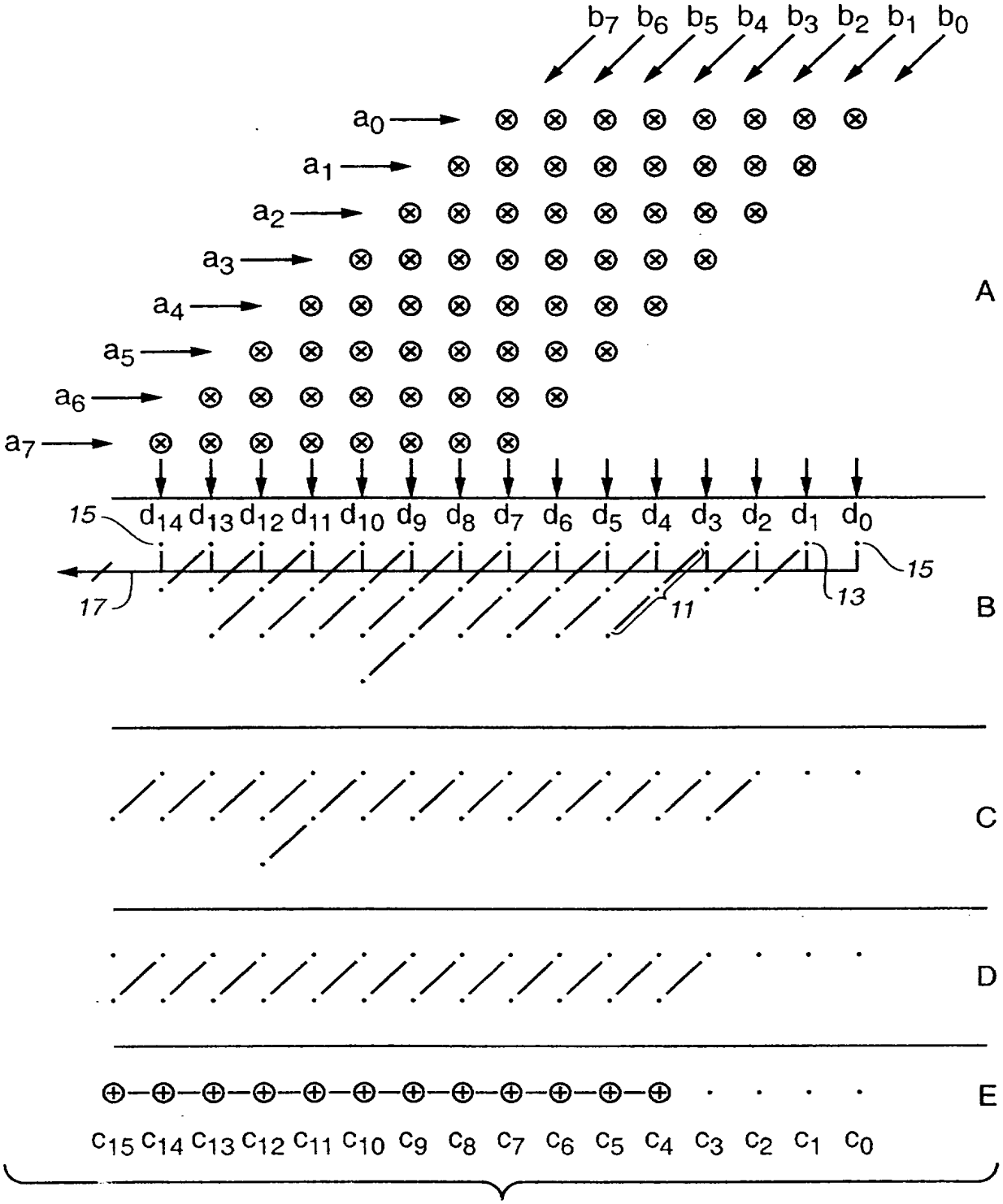
b7 b6 b5 b4 b3 b2 b1 b0
a0
a1
a2
a3
a4
a5
a6
a7
A
15
d14 d13 d12 d11 d10 d9 d8 d7 d6 d5 d4 d3 d2 d1 d0
15
17
11
13
B
C
D
E
c15 c14 c13 c12 c11 c10 c9 c8 c7 c6 c5 c4 c3 c2 c1 c0

FIG._2

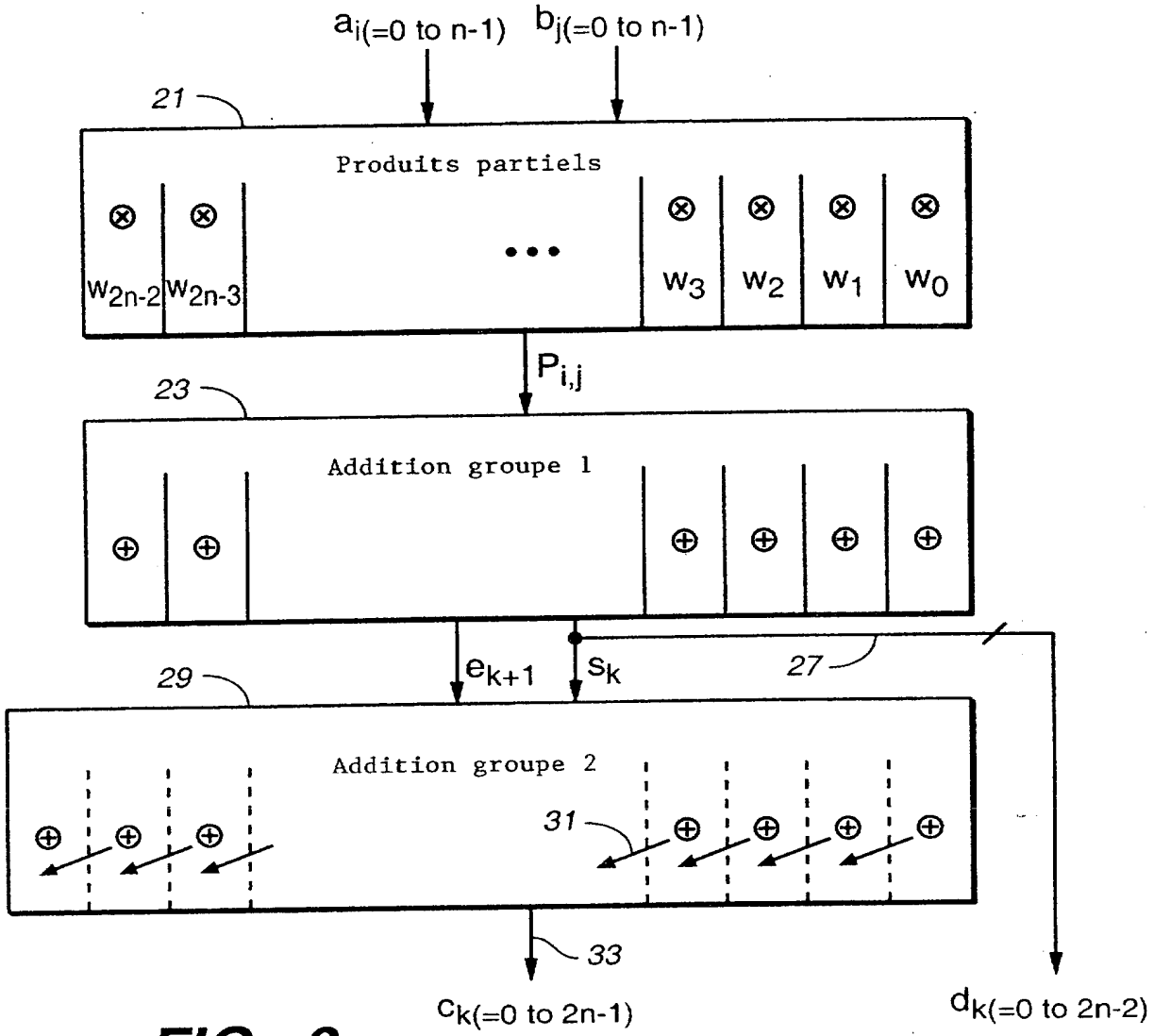
$a_{i(=0 \text{ to } n-1)}$
$b_{j(=0 \text{ to } n-1)}$
21
Produits partiels
w_{2n-2}
w_{2n-3}
w_3
w_2
w_1
w_0
$P_{i,j}$
23
Addition groupe 1
e_{k+1}
s_k
27
29
Addition groupe 2
31
33
$c_{k(=0 \text{ to } 2n-1)}$
$d_{k(=0 \text{ to } 2n-2)}$

FIG._3

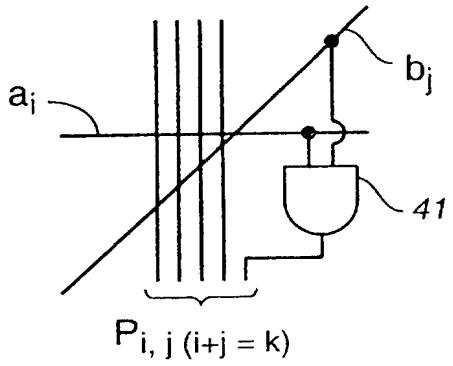
a_i
b_j
41
$P_{i,\ j\ (i+j\ =\ k)}$

FIG._4

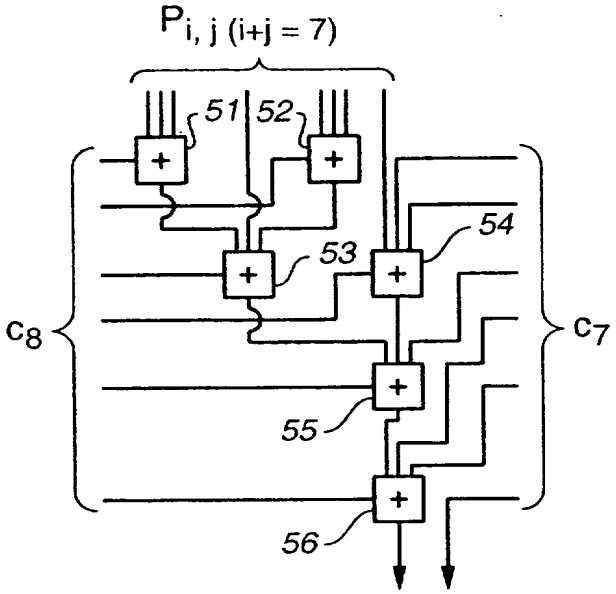

FIG._5

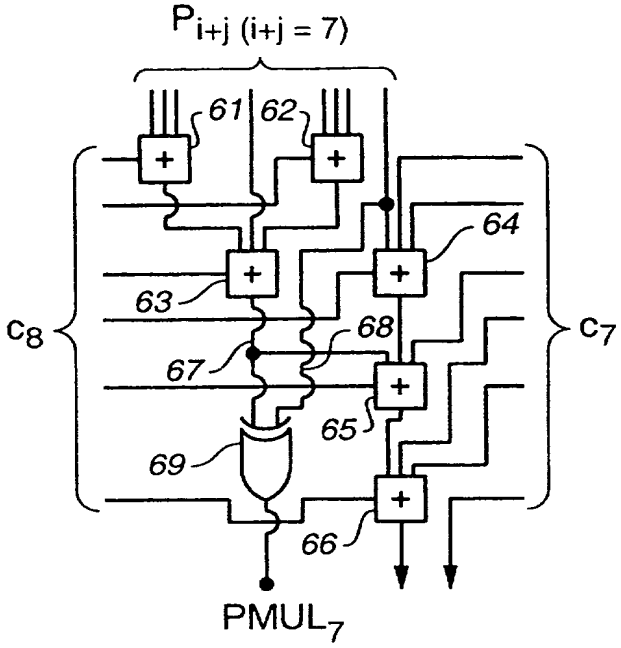

FIG._6

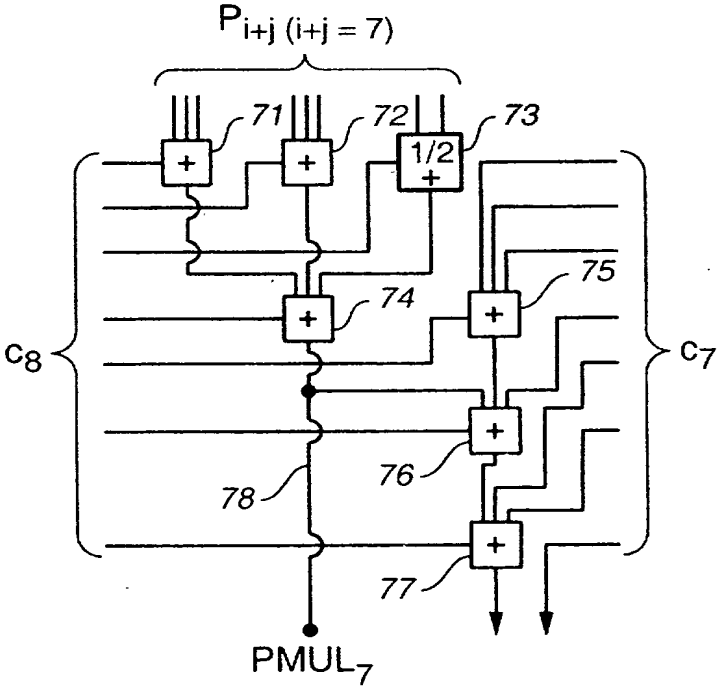

FIG._7

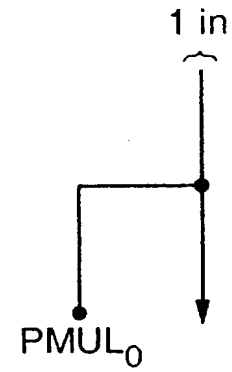

FIG._8A

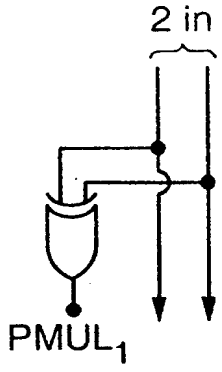

FIG._8B

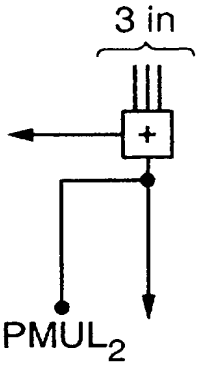

FIG._8C

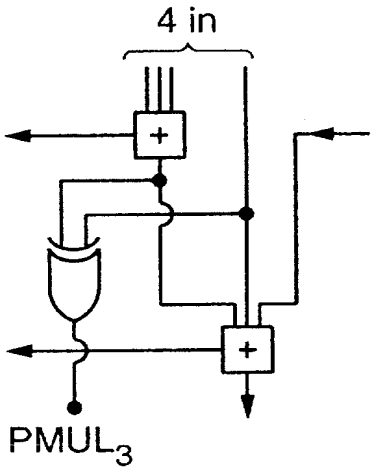

FIG._8D

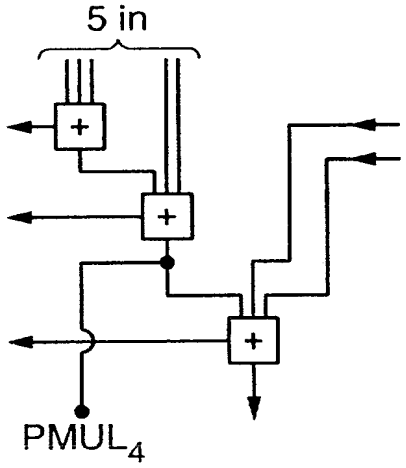

FIG._8E

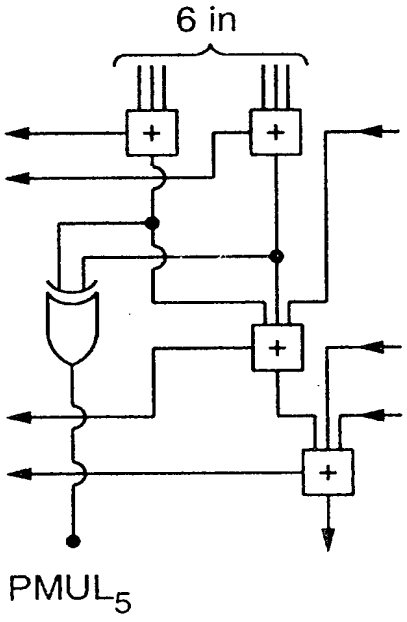

FIG._8F

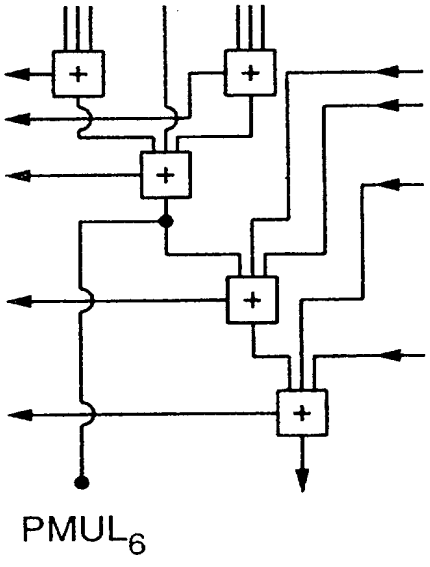

FIG._8G

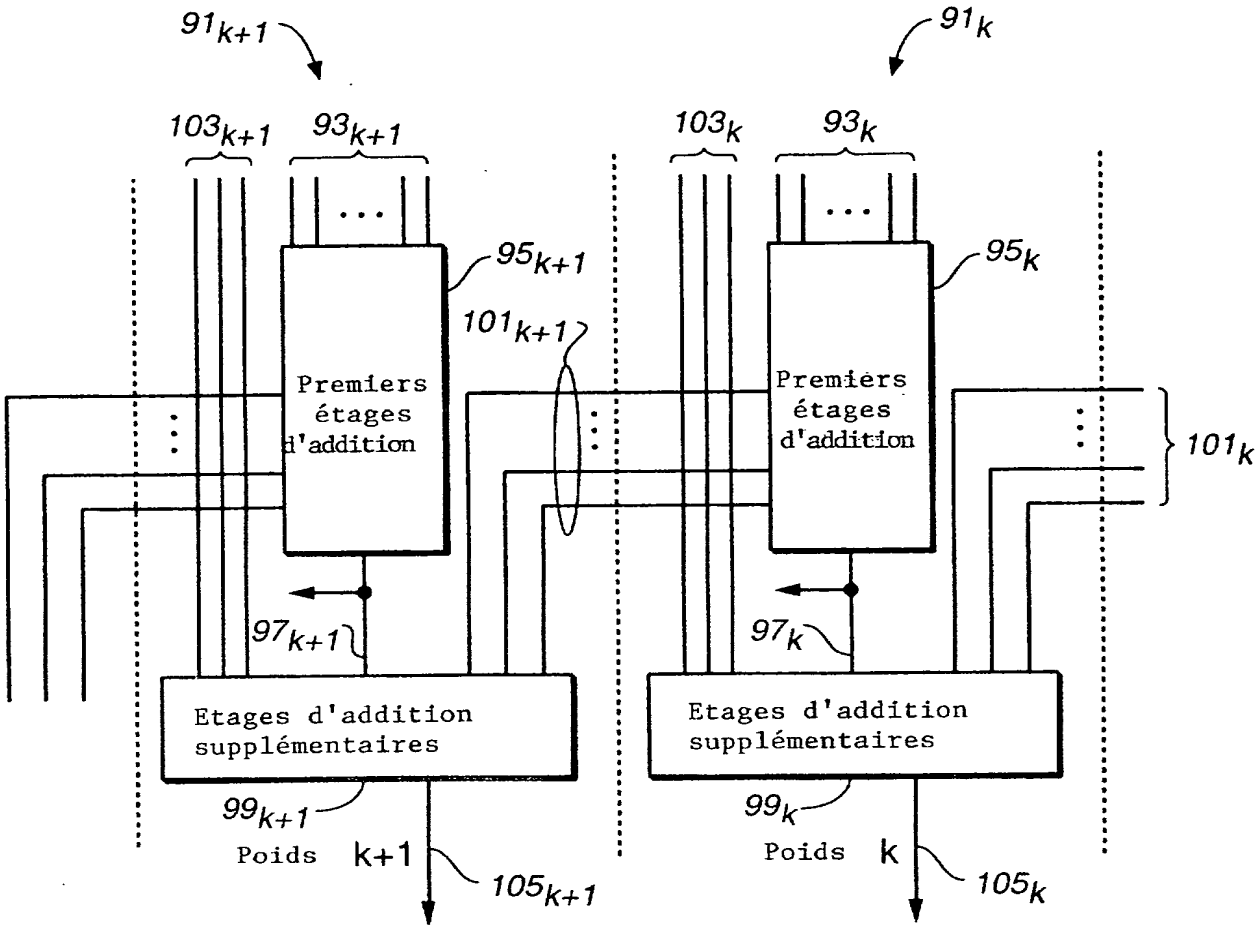
91_{k+1}
91_k
103_{k+1}
93_{k+1}
103_k
93_k
95_{k+1}
95_k
101_{k+1}
Premiers étages d'addition
Premiers étages d'addition
101_k
97_{k+1}
97_k
Etages d'addition supplémentaires
Etages d'addition supplémentaires
99_{k+1}
99_k
Poids k+1
Poids k
105_{k+1}
105_k

FIG._9

reçue le 13/05/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	33299/FR
N° D'ENREGISTREMENT NATIONAL	0304221

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

ARCHITECTURE DE MULTIPLICATEURS POLYNOMIAL ET NATUREL COMBINES

LE(S) DEMANDEUR(S) :

Atmel Corporation
2325 Orchard Parkway
SAN JOSE California 95131
U.S.A.

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		DUPAQUIS
Prénoms		Vincent
Adresse	Rue	4 rue du Collet
	Code postal et ville	13124 PEYPIN
Société d'appartenance *(facultatif)*		
2 Nom		PARIS
Prénoms		Laurent
Adresse	Rue	28 Le Ribas
	Code postal et ville	13790 ROUSSET
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Le 04/04/2003

BRESSE Pierre 92103B

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.